Europ. J. Combinatorics (1992) **13**, 335–343

How Far Apart Can the Group Multiplication Tables be?

ALEŠ DRÁPAL

Put $\mathrm{dist}(G(\cdot), G(*)) = \mathrm{card}\{(a, b) \in G^2; a \cdot b \neq a * b\}$ for any two groups $G(\cdot)$, $G(*)$ with the same underlying set and $\delta(G(\cdot)) = \min \mathrm{dist}(G(\cdot), G(*))$, where $G(*)$ runs through all groups with $\mathrm{dist}(G(\cdot), G(*)) \neq 0$. It holds that $\delta(G(\cdot)) \in \{6n - 24, 6n - 20, 6n - 18\}$ for any $n \geq 51$, n being the order of G. Moreover, groups $G(\cdot)$ and $G(*)$ are isomorphic whenever $\mathrm{dist}(G(\cdot), G(*)) \leq n^2/9$.

1. INTRODUCTION

Combinatorial problems concerning finite groups seem to split into two categories: either their solution is more or less straightforward, or rather deep structural knowledge of finite groups is required. This is also true for problems involving the group multiplication table (the Cayley table); as an example one may cite the well known problem of finding a transversal in the multiplication table of a finite group [5].

In this paper we shall consider the following question. Let $G(\cdot)$ and $G(*)$ be two groups of order $n \geq 2$ defined on the same underlying set G. The number $\mathrm{card}\{(a, b) \in G^2; a \cdot b \neq a * b\}$ is said to be their (Hamming) *distance* and will be denoted by $\mathrm{dist}(G(\cdot), G(*))$. For any group $G(\cdot)$ we define $\delta(G(\cdot)) = \min \mathrm{dist}(G(\cdot), G(*))$, with $G(*)$ running through all groups on G, $G(*) \neq G(\cdot)$. What can be said about $\delta(G(\cdot))$?

We prove that $\delta(G(\cdot)) \in \{6n - 24, 6n - 20, 6n - 18\}$ for $n \geq 51$. We also prove that the groups $G(\cdot)$ and $G(*)$ are isomorphic if $\mathrm{dist}(G(\cdot), G(*)) < n^2/9$. In other words, whenever $G(\cdot)$ is a group on G and $G(*)$ runs through all groups on G that are non-isomorphic to $G(\cdot)$, then $\nu(G(\cdot)) = \min \mathrm{dist}(G(\cdot), G(*)) > n^2/9$. This estimate of $\nu(G(\cdot))$ is probably not sharp enough as no example of non-isomorphic groups $G(\cdot)$ and $G(*)$ with $\mathrm{dist}(G(\cdot), G(*)) < n^2/4$ seems to be known. Unfortunately, to obtain a better estimate of $\nu(G(\cdot))$ seems to be beyond the power of the tools employed in this paper.

Note that a related problem has been solved by Dénes [1–3]: For a group $G(\cdot)$ put $\mu(G(\cdot)) = \min \mathrm{dist}(G(\cdot), G(*))$, with $G(*) \neq G(\cdot)$ running through all quasi-groups which are isotopic to a group on G. Then $\mu(G(\cdot)) = 2n$, except for the case of $G(\cdot)$ abelian of order 4 or 6. In these exceptional cases $\mu(G(\cdot))$ equals 4 or 9, respectively.

Note also that the methods employed here are in some aspects similar to the methods used in [4].

2. TILTING SEQUENCES

Throughout this paper, $G(\cdot)$ and $G(*)$ denote two distinct groups of order $n \geq 2$. Inverse elements in $G(\cdot)$ are denoted by g^{-1}, while those in $G(*)$ are denoted by g^*.

We define $\pi_i: G^2 \to G$, $1 \leq i \leq 4$ by $\pi_1(a, b) = a$, $\pi_2(a, b) = b$, $\pi_3(a, b) = a \cdot b$, $\pi_4(a, b) = a * b$. Furthermore, for $1 \leq i < j \leq 4$ we put $\pi_{ij}(a, b) = (\pi_i(a, b), \pi_j(a, b))$. Observe that:

LEMMA 2.1. (i) *π_{ij} is a permutation of G^2 for any $1 \leq i < j \leq 4$, $(i, j) \neq (3, 4)$.*
(ii) *For any $a \in G$, $1 \leq i, j \leq 4$, $i \neq j$, $\{i, j\} \neq \{3, 4\}$, the restriction of π_i to $\pi_j^{-1}(\{a\})$ bijects $\pi_j^{-1}(\{a\})$ onto G.*

0195-6698/92/050335 + 09 $08.00/0

We put $M = \{(a, b) \in G^2; a \cdot b \neq a * b\}$ and $m = \mathrm{card}(M) = \mathrm{dist}(G(\cdot), G(*))$. For $1 \leq i \leq 4$ and $a \in G$ we define $p_i(a) = \mathrm{card}\{\pi_i^{-1}(\{a\}) \cap M\}$. Obviously, the following holds:

LEMMA 2.2. (i) $\sum_{a \in G} p_i(a) = m$ *for any* $1 \leq i \leq 4$.
(ii) $p_3(a) = p_4(a)$ *for all* $a \in G$.

In the following we shall often deal with terms where operations $\cdot$ and $*$ appear together. To this purpose we define $W(X)$ to be the absolutely free algebra over a (non-empty) set X with the binary operations $\cdot$ and $*$, and the unary operations $^{-1}$ and *.

Two terms t_1, t_2 are said to be *linked* by $(w_1, w_2) \in W(X)^2$ iff t_1 can be obtained from t_2 by substituting its subterm $w_1 \cdot w_2$ by $w_1 * w_2$ (or vice versa). More formally:
(i) $(w_1, w_2) \in W(X)^2$ links $w_1 \cdot w_2$ with $w_1 * w_2$ and $w_1 * w_2$ with $w_1 \cdot w_2$;
(ii) if t_1, t_2 are linked by $(w_1, w_2) \in W(X)^2$ and $t \in W(X)$, then (w_1, w_2) links s_1 with s_2 whenever $(s_1, s_2) \in \{(t \cdot t_1, t \cdot t_2), (t * t_1, t * t_2), (t_1 \cdot t, t_2 \cdot t), (t_1 * t, t_2 * t), (t_1^{-1}, t_2^{-1}), (t_1^*, t_2^*)\}$.

For $t_1, t_2 \in W(X)$ we write $t_1 \sim t_2$ iff for any groups $H(\cdot)$, $H(*)$ defined on a set H and for any homomorphism $\varphi: W(X) \to H(\cdot, *)$ it holds that $\varphi(t_1) = \varphi(t_2)$. The relation $\sim$ is obviously a congruence and $W(X)/\sim$ could be called a free bigroup over X.

We shall now assume that $X = \{x, y\} \cup Z$, $Z = \{z_1, \ldots, z_r\}$ is finite and $\mathrm{card}(X) = r + 2$.

A finite sequence $\tau = (\tau_i)$, $1 \leq i \leq k$, $\tau_i = (t_{i,1}, t_{i,2}) \in W(X)^2$ is said to be a *tilting sequence* iff:
(i) $t_{1,1} = x \cdot y$ and $t_{k,2} = x * y$;
(ii) $t_{i,1} \sim t_{i,2}$ for any $1 \leq i \leq k$;
(iii) $t_{i,2}$ and $t_{i+1,1}$ are linked by some $(w_{i,1}, w_{i,2}) \in W(X)^2$ for any $1 \leq i \leq k - 1$.

For each $1 \leq i \leq k - 1$ the groups $G(\cdot)$ and $G(*)$ induce a *tilting mapping* τ_i': $G^{r+2} \to G^2$, $\tau_i'(a, b, c_1, \ldots, c_r) = (\varphi(w_{i,1}), \varphi(w_{i,2}))$, where $\varphi: W(X) \to G(\cdot, *)$ is the homomorphism determined by $\varphi(x) = a$, $\varphi(y) = b$, $\varphi(z_j) = c_j$, $1 \leq j \leq r$.

LEMMA 2.3. *Let* $\tau = (\tau_i)$, $1 \leq i \leq k$ *be a tilting sequence and let* $(a, b) \in M$. *Then for any* $(c_1, \ldots, c_r) \in G^r$ *there exists* $1 \leq s \leq k - 1$ *with* $\tau_s'(a, b, c_1, \ldots, c_r) \in M$.

PROOF. Assume the contrary and consider the homomorphism $\varphi: W(X)^2 \to G(\cdot, *)$ determined by $\varphi(x) = a$, $\varphi(y) = b$, $\varphi(z_j) = c_j$, $1 \leq j \leq r$. Then $\varphi(w_{i,1} * w_{i,2}) = \varphi(w_{i,1} \cdot w_{i,2})$ for any $1 \leq i \leq k - 1$ and thus $\varphi(t_{i,2}) = \varphi(t_{i+1,1})$. Hence $a \cdot b = \varphi(t_{i,1}) = \varphi(t_{k,2}) = a * b$, a contradiction. □

In the following we shall use the tilting sequences α and β. There are $r = 1$ and $k = 4$ in the both sequences, and we put $z = z_1$. We define

$$\alpha_1 = (x \cdot y, ((x \cdot y) * z) * z^*), \qquad \alpha_2 = (((x \cdot y) \cdot z) * z^*, (x \cdot (y \cdot z)) * z^*),$$
$$\alpha_3 = ((x * (y \cdot z)) * z^*, x * ((y \cdot z) * z^*)), \qquad \alpha_4 = (x * ((y * z) * z^*), x * y)$$

and

$$\beta_1 = (x \cdot y, (x \cdot (y \cdot z^{-1})) \cdot z), \qquad \beta_2 = ((x \cdot (y \cdot z^{-1})) * z, (x \cdot (y \cdot z^{-1})) * z),$$
$$\beta_3 = ((x * (y \cdot z^{-1})) * z, x * ((y \cdot z^{-1}) * z)), \qquad \beta_4 = (x * ((y \cdot z^{-1}) \cdot z), x * y).$$

The tilting mappings α_i', β_i', $1 \leq i \leq 3$ are thus given by $\alpha_1'(a, b, g) = (ab, g)$, $\alpha_2'(a, b, g) = (a, bg)$, $\alpha_3'(a, b, g) = (b, g)$ and $\beta_1'(a, b, g) = (abg^{-1}, g)$, $\beta_2'(a, b, g) = (a, bg^{-1})$, $\beta_3'(a, bg) = (bg^{-1}, g)$.

For $A \subseteq M$ consider the set $B = \bigcup \alpha_i'(A \times G)$, $1 \leqslant i \leqslant 3$. Lemma 2.3 provides a reason to believe that the set $B \cap M$ will be large relative to A, when A is small. Pursuing this idea for A containing just a single pair $(a, b) \in M$ and for $A = M \cap \pi_1^{-1}(\{a\})$, $a \in G$, we shall obtain the important inequalities of 2.4, 4.1 and 8.1.

Postponing the case of G infinite to Section 8, we shall assume now that $G(\cdot)$ is a finite group of order n.

LEMMA 2.4. *For any $(a, b) \in M$ it holds that $n \leqslant p_1(a) + p_1(b) + p_1(ab)$, $n \leqslant p_2(a) + p_2(b) + p_2(ab)$, $n \leqslant p_1(a) + p_3(b) + p_3(ab)$ and $n \leqslant p_3(a) + p_2(b) + p_3(ab)$.*

PROOF. To prove the first inequality, consider the sets $S_i = \{g \in G;\ \alpha_i'(a, b, g) \in M\}$, $1 \leqslant i \leqslant 3$. By 2.3 it is $\bigcup S_i = G$ and we see that $S_1 = \pi_2(\pi_1^{-1}(\{ab\}) \cap M)$, $S_3 = \pi_2(\pi_1^{-1}(\{b\}) \cap M)$ and $S_2 = \lambda_b^{-1}\pi_2(\pi_1^{-1}(\{a\}) \cap M)$, λ_b being the translation $g \mapsto b \cdot g$ of $G(\cdot)$. By 2.1(ii) we have $p_1(ab) = \mathrm{card}(S_1)$, $p_1(b) = \mathrm{card}(S_3)$ and $p_1(a) = \mathrm{card}(S_2)$.

To prove the third inequality, put $T_i = \{g \in G;\ \beta_i'(a, b, g) \in M\}$, $1 \leqslant i \leqslant 3$. Then $T_1 = \pi_2(\pi_3^{-1}(\{ab\}) \cap M)$, $T_3 = \pi_2(\pi_3^{-1}(\{b\}) \cap M)$ and $T_2^{-1} = \lambda_b^{-1}\pi_2(\pi_1^{-1}(\{a\}) \cap M)$.

The other two inequalities can be obtained from the already proved ones by applying them to the opposite groups $G^{op}(\cdot)$ and $G^{op}(*)$. □

3. CONSTRUCTING AN ISOMORPHISM

PROPOSITION 3.1. *Let $G(\cdot)$ and $G(*)$ be two groups on the finite set G, $\mathrm{card}(G) = n$. Put $K = \{a \in G;\ p_1(a) < n/3\}$ and suppose that $\mathrm{card}(K) > 3n/4$. Define a mapping f of G onto itself by $f(g) = a * b$ for any $g \in G$, $a, b \in K$, $g = a \cdot b$. Then f is an isomorphism of $G(\cdot)$ onto $G(*)$, and $f(a) = a$ for $a \in K$. Moreover, $f(g) \neq g$ for any $g \in G$ with $p_1(g) > 2n/3$.*

PROOF. We divide the proof into several steps:

(i) First, observe that given arbitrary sets $K_i \subseteq G$, $1 \leqslant i \leqslant 4$, $\mathrm{card}(K_i) \geqslant \mathrm{card}(K)$, it always holds $\bigcap K_i \neq \emptyset$.

(ii) Let $a, b \in G$ be such that $\{a, b, ab\} \subseteq K$. Then $p_1(a) < n/3$, $p_1(b) < n/3$, $p_1(ab) < n/3$ and so $n < p_1(a) + p_1(b) + p_1(ab)$ is impossible. Therefore $ab = a * b$ by 2.4.

(iii) By induction, $a_1 a_2 \cdots a_k = a_1 * a_2 * \cdots * a_k$ whenever $a_i \in K$, $1 \leqslant i \leqslant k$ are such that $a_1 a_2 \cdots a_i \in K$ for any $2 \leqslant i \leqslant k$.

(iv) Since $\mathrm{card}(K) > n/2$, each $g \in G$ can be expressed as $g = ab$, $a, b \in K$. Let $g = a_i b_i$, $1 \leqslant i \leqslant 2$, $a_i, b_i \in K$. The set $K \cap Kg^{-1} \cap Ka_1^{-1} \cap Ka_2^{-1}$ is non-empty by (i), and hence there exists $c \in K$ with $cg \in K$, $ca_1 \in K$ and $ca_2 \in K$. Then $c \in K$, $a_i \in K$, $b_i \in K$, $ca_i \in K$, $ca_i b_i \in K$ and by (iii) $cg = ca_i b_i = c * a_i * b_i$, which implies $a_1 * b_1 = a_2 * b_2 = f(g)$. This proves that the mapping f has been defined correctly.

(v) Let $a \in K$ and $g \in G$ be such that $ag \in K$. Since $\mathrm{card}(K) > 2n/3$, g clearly has more than $n/3$ representations as a product $g = bc$ with $b, c \in K$. But having more than $n/3$ choices for b implies that we can choose $b \in K$ so that $ab \in K$ as well. With b, c so chosen, we have a, b, c, ab and $ag = abc$ all in K. Then $a * b * c = abc$ by (iii), and this proves that $a * f(g) = a \cdot g$ whenever $a \in K$, $g \in G$ and $a \cdot g \in K$.

(vi) Suppose that $f(g_1) = f(g_2)$ for some $g_i \in G$, $i = 1, 2$. Then there exists $a \in K$ with $ag_i \in K$ and by (v) we have $ag_i = a * f(g_i)$. This implies $g_1 = g_2$ and f is a permutation.

(vii) Let now $g, h \in G$ be arbitrary and choose $a \in K$ with $ag \in K$, $agh \in K$. Then $a * f(g) * f(h) = (ag) * f(h) = agh = a * f(gh)$ by (v). Therefore $f(g \cdot h) = f(g) * f(h)$ and we have proved that f is an isomorphism.

(viii) Any $a \in K$ can be expressed as $a = b \cdot c$ with $b, c \in K$, and thus $f(a) = a$ follows from (ii). Conversely, let $g \in G$ be such that $p_1(g) \geq 2n/3$. Then $g * b \neq g \cdot b$ for at least $2n/3$ choices of b, and from $\mathrm{card}(K) > 2n/3$, $\mathrm{card}(g^{-1}K) > 2n/3$ it follows that there exists $b \in K$ with $gb \in K$ and $g * b \neq gb$. Therefore $gb = f(gb) = f(g) * f(b) = f(g) * b \neq g * b$, and hence $f(g) \neq g$.

Note that $\mathrm{card}(K) > 3n/4$ is in fact required only in the proof of (iv). Elsewhere it is enough to assume $\mathrm{card}(K) > 2n/3$.

4. Inequalities

Lemma 4.1. *$2m \geq p_1(a)(n - p_1(a)) + p_1(a)$ for any $a \in G$.*

Proof. Put $P = \pi_1^{-1}(\{a\}) \cap M$; by definition we have $\mathrm{card}(P) = p_1(a)$. Furthermore, put $J = \{x \in P \times G;\ \alpha_i'(x) \in P \text{ for no } 1 \leq i \leq 3\}$ and $K_i = \{x \in P \times G;\ \alpha_i'(x) \in P\}$, $K = \bigcup K_i$, $1 \leq i \leq 3$. Clearly, $K \cap J = \emptyset$ and $K \cup J = P \times G$. Now consider the set $L = M \cap (\alpha_1'(J) \cup \alpha_2'(J) \cup \alpha_3'(J))$. By the definitions of J and α_2' we have $\alpha_2'(J) \cap M = \emptyset$, and hence $L = M \cap (\alpha_1'(J) \cup \alpha_3'(J))$. The tilting mappings α_1' and α_3' are injective on $P \times G \supseteq J$ and from 2.3 we obtain $\alpha_1'(x) \in M$ or $\alpha_3'(x) \in M$ for each $x \in J$. Thus $J = \{x \in J;\ \alpha_1'(x) \in M\} \cup \{x \in J;\ \alpha_3'(x) \in M\}$, and there exists $j \in \{1, 3\}$ with $\mathrm{card}(L) \geq \mathrm{card}\{x \in J;\ \alpha_j'(x) \in M\} \geq \mathrm{card}(J)/2$. From $L \cap P = \emptyset$ we now obtain $m \geq \mathrm{card}(P) + \mathrm{card}(L) \geq p_1(a) + \mathrm{card}(J)/2 = p_1(a) + (np_1(a) - \mathrm{card}(K))/2$. Thus $2m \geq np_1(a) + p_1(a) - (\mathrm{card}(K) - p_1(a))$ and it remains to prove that $\mathrm{card}(K) \leq p_1(a) + p_1^2(a)$.

First, note that $x = (a, b, g) \in K_1$ only when $(ab, g) \in P$, which implies $b = 1$ and $\alpha_2'(x) = (a, bg) \in P$. Thus $K_1 \subseteq K_2$, and it suffices to prove $\mathrm{card}(K_3) \leq p_1(a)$ and $\mathrm{card}(K_2) \leq p_1^2(a)$.

However, we have $(b, g) = \alpha_3'(a, b, g) \in P$ iff $a = b$. Thus $\mathrm{card}(K_3) = p_1(a)$ if $(a, a) \in M$ and $\mathrm{card}(K_3) = 0$ when $(a, a) \notin M$.

By 2.1(ii) we have $p_1(a) = \mathrm{card}(\pi_2(P))$ and for each c, $b \in \pi_2(P)$ there exists exactly one $g \in G$ with $(a, c) = (a, bg) = \alpha_2'(a, b, g) \in P$. Thus $\mathrm{card}(K_2) = p_1^2(a)$. □

Lemma 4.2. *Let r, t be real numbers such that $0 < r < \frac{1}{8}$, $0 < t < \frac{1}{2}$ and $2r = \frac{1}{4} - t^2$. Suppose that $m \leq rn^2$. Then for any $g \in G$ we have either $p_1(g) < (\frac{1}{2} - t)n$, or $p_1(g) > (\frac{1}{2} + t)n$.*

Proof. Assume the contrary. Then $(\frac{1}{2} - t)n \leq p_1(g) \leq (\frac{1}{2} + t)n$ for some $g \in G$ and

$$m \leq rn^2 = \tfrac{1}{2}(\tfrac{1}{4} - t^2)n^2 = \tfrac{1}{2}((\tfrac{1}{2} - t)n(\tfrac{1}{2} + t)n) \leq \tfrac{1}{2}p_1(g)(n - p_1(g)) < m,$$

a contradiction. □

Remark 4.3. Under the assumptions of 4.2 one can in fact prove that for any $g \in G$ either $p_i(g) < (\frac{1}{2} - t)n$ for all $1 \leq i \leq 3$, or $p_i(g) > (\frac{1}{2} + t)n$ for all $1 \leq i \leq 3$. This follows easily from the fact that for any $1 \leq i, j \leq 3$ and any $g \in G$ it holds that $2m \geq p_i(g)(n - p_j(g)) + p_j(g)$. In 4.1 we have proved one of these nine inequalities, and the others can be proved in a similar manner. However, for our purposes this is not necessary.

Lemma 4.4. *Let L be a subset of G, $l = \mathrm{card}(L)$ and s a real number, $\frac{1}{2} < s \leq 1$. Suppose that $p_i(a) > sn$ for each $a \in L$, $1 \leq i \leq 3$. Then $3l(sn - l) < m$.*

Proof. For $1 \leq i \leq 3$ let $P_i = \pi_i^{-1}(L) \cap M$. Then $M \supseteq P_i$ and we have $m \geq \sum_{1 \leq i \leq 3} \mathrm{card}(P_i) - \sum_{1 \leq i < j \leq 3} \mathrm{card}(P_i \cap P_j)$. However, $\mathrm{card}(P_i) \geq \mathrm{card}(L) \cdot \min\{p_i(a);\ a \in L\} > l \cdot sn$ and as $\pi_{ij}(P_i \cap P_j) \subseteq L \times L$, we have $\mathrm{card}(P_i \cap P_j) \leq l^2$ by 2.1(i).

PROPOSITION 4.5. *Suppose that $G(\cdot)$ is a finite group of order n, and $G(*)$ another group on G. The groups $G(\cdot)$ and $G(*)$ are isomorphic, if* $\operatorname{dist}(G(\cdot), G(*)) \leq n^2/9$. *In such a case there exists an isomorphism f with* $\operatorname{card}(\{g \in G; f(g) \neq g\}) < n/16$.

PROOF. Put $K = \{g \in G; p_1(g) < n/3\}$, $L = \{g \in G; p_1(g) > 2n/3\}$, $l = \operatorname{card}(L)$ and suppose that $0 < m = \operatorname{dist}(G(\cdot), G(*)) \leq n^2/9$. Using 4.2 for $t = \frac{1}{6}$ and $r = \frac{1}{9}$, we obtain $K \cup L = G$. There is $n^2/9 \geq m \geq \sum_{g \in L} p_1(g) > 2nl/3$, and thus $n > 6l$. By 3.1 there exists an isomorphism f with $f(g) \neq g$ just for $g \in L$. We have $a * b = f(f^{-1}(a)f^{-1}(b)) \neq ab$ whenever $a \in K$, $b \in K$, $ab \in L$, or $a \in K$, $b \in L$ and $ab \in K$. As $\operatorname{card}(K \cap K^{-1}g) \geq n - 2l > 2n/3$ for any $g \in G$, there exist more than $2n/3$ pairs $(a, b) \in K^2$ with $ab = g$. Hence $p_3(g) > 2n/3$ for any $g \in L$ and, similarly, we obtain $p_2(g) > 2n/3$ for any $g \in L$. Now we can use 4.4 with $s = \frac{2}{3}$, and for $\lambda = l/n$ we obtain $\lambda(2 - 3\lambda) < \frac{1}{9}$. It follows that $\lambda < (3 - \sqrt{6})/9 < \frac{1}{16}$. □

5. ISOMORPHIC GROUPS

We have proved in 4.5 that the groups with small distance are isomorphic. Therefore we shall assume throughout this section that $a * b = f^{-1}(f(a) \cdot f(b))$ for a permutation f of G and we shall investigate how the number $m = m_f = \operatorname{dist}(G(\cdot), G(*))$ depends on f. We put $K = K_f = \{g \in G; f(g) = g\}$, $k = k_f = \operatorname{card}(K_f)$, $L = L_f = \{g \in G; f(g) \neq g\}$ and $l = l_f = \operatorname{card}(L_f)$. Obviously, $K_f \cap L_f = \emptyset$ and $k_f + l_f = n$.

For A, B, C subsets of G let $m_f(A, B, C) = \operatorname{card}(\{(a, b) \in A \times B; ab \in C$ and $f(a)f(b) \neq f(ab)\})$ and $d(A, B, C) = \operatorname{card}(\{(a, b) \in A \times B; ab \in C\})$. Clearly, $m_f(A, B, C) \leq d(A, B, C)$.

LEMMA 5.1. *It holds that* $m_f = m_f(G, G, G) = \operatorname{card}\{(a, b) \in G^2; f(a)f(b) \neq f(ab)\}$. *Furthermore,* $m_f(K, K, K) = 0$, $m_f(K, K, L) = d(K, K, L)$, $m_f(K, L, K) = d(K, L, K)$, $m_f(L, K, K) = d(L, K, K)$, *and hence* $d(K, K, L) + d(K, L, K) + d(L, K, K) \leq m_f = d(K, K, L) + d(K, L, K) + d(L, K, K) + m_f(K, L, L) + m_f(L, K, L) + m_f(L, L, K) + m_f(L, L, L) \leq n^2 - d(K, K, K)$.

PROOF. We have $a * b = ab$ iff $f(ab) = f(a) \cdot f(b)$, Hence $a * b = ab$ for $\{a, b, ab\} \subseteq K$, and thus $m_f(K, K, K) = 0$. Furthermore, $f(ab) \neq ab = f(a)f(b)$ for $a \in K$, $b \in K$ and $ab \in L$, and thus $m_f(K, K, L) = d(K, K, L)$. The rest is similar. □

LEMMA 5.2. *Suppose that $G(\circ)$ is a quasi-group defined on G, and S a subset of G,* $s = \operatorname{card}(S)$. *Put* $d = \operatorname{card}\{(a, b) \in S^2; a \circ b \in S\}$ *and* $R = G \setminus S$. *Then* $\operatorname{card}\{(a, b) \in R^2; a \circ b \in R\} = n^2 - 3s(n - s) - d \geq n^2 - s(3n - 2s)$ *and* $\operatorname{card}\{(a, b) \in R^2; a \circ b \in S\} = s(n - 2s) + d \geq s(n - 2s)$.

PROOF. For $r_1 = \operatorname{card}\{(a, b) \in R^2; a \circ b \in R\}$, $s_1 = \operatorname{card}\{(a, b) \in R^2; a \circ b \in S\}$ and $s_2 = \operatorname{card}\{(a, b) \in R \times S; a \circ b \in S\}$ it holds that $r_1 + s_1 = (n - s)^2$, $s_1 + s_2 = s(n - s)$ and $s_2 + d = s^2$.

COROLLARY 5.3. *We have* $d(K, K, L) = l(n - 2l) + d(L, L, L)$, $d(K, L, K) = l(n - 2l) + d(L^{-1}, L, L)$, $d(L, K, K) = l(n - 2l) + d(L, L^{-1}, L)$ *and* $d(K, K, K) = n^2 - 3l(n - l) - d(L, L, L)$.

PROOF. To obtain the first and the last equality, use 5.2 with $a \circ b = ab$. The second and the third equality follow from 5.2 when we put $a \circ b = a^{-1}b$ and $a \circ b = ab^{-1}$, respectively.

COROLLARY 5.4. $9kn - 3n^2 - 6k^2 = 3ln - 6l^2 \leqslant m_f \leqslant 3ln - 2l^2 = n^2 + kn - 2k^2$.

PROOF. Combine 5.1 and 5.3.

PROPOSITION 5.5. *For a finite group G of order n and a subset L of G, $l = \mathrm{card}(L) \geqslant 2$, let F_L denote the set of all permutations f of G, which have $f(a) \neq a$ just for $a \in L$. Then*:
(i) *$m_f = 3ln - 6l^2$ for some $f \in F_L$ iff $ab \in L$, $ab^{-1} \in L$, $a^{-1}b \in L$ for no $a, b \in L$, and there exists $h \in G$ such that $hL = L = Lh$, $h \neq 1$, and $hah = a$ for each $a \in L$;*
(ii) *$m_f = 3ln - 2l^2$ for some $f \in F_L$ iff L is a subgroup of G.*

PROOF. (i) Suppose that $f \in F_L$ is such that $m_f = 3ln - 6l^2$. Then $d(L, L, L) = d(L^{-1}, L, L) = d(L, L^{-1}, L) = 0 = m_f(L, L, K)$ by 5.3 and 5.1. Therefore $f(a)f(b) = ab \in K$ for every $a, b \in L$, and $a^{-1}f(a) = h$ is thus constant for all $a \in L$. Putting $a = b$ we obtain $a = a^{-1}f(a)f(a) = hah$, and from $f(L) = L$ we have $L = Lh = hLh = hL$. Conversely, suppose that L and h satisfy the hypothesis of (i). Define $f \in F_L$ by $f(a) = ah = h^{-1}a$ for every $a \in L$. Then $f(a)f(b) = ahh^{-1}b = ab$, $(f(a))^{-1}f(b) = a^{-1}hh^{-1}b = a^{-1}b$ and $f(a)(f(b))^{-1} = ahh^{-1}b^{-1} = ab^{-1}$ for any $a, b \in L$. Consequently, $m_f(L, L, K) = m_f(K, L, L) = m_f(L, K, L) = 0 = d(L, L, L) = d(L, L^{-1}, L) = d(L^{-1}, L, L)$.
(ii) By 5.3 and 5.1 we have $m_f \leqslant 3l(n - l) + d(L, L, L)$, and thus $m_f = 3l(n - l) + l^2$ implies that L is a subgroup of G. Conversely, given a subgroup L of G and $f \in F_L$, we have $d(L^{-1}, L, L) = d(L, L^{-1}, L) = d(L, L, L) = l^2$ and $d(K, L, L) = d(L, K, L) = d(L, L, K) = 0$. Hence $m_f = 3ln - 3l^2 + m_f(L, L, L)$, and we can achieve $m_f(L, L, L) = l^2$ so that we choose $1 \neq h \in L$ and put $f(a) = ah$ for all $a \in L$. □

COROLLARY 5.6. *Let H be a subgroup of G, $l > 1$ the order of H, $g \in G \setminus H$ and let $L = gH$. Then there exists $f \in F_L$ with $m_f = 3ln - 6l^2$ iff H contains such an element $h \neq 1$ that $h^{-1} = g^{-1}hg$ and $ha = ah$ for all $a \in H$.*

PROOF. Obviously, $ab \in L$, $ab^{-1} \in L$, $a^{-1}b \in L$ for no $a, b \in L$. If $f \in F_L$ and $m_f = 3ln - 6l^2$, then there exists $h \in G$ with $gHh = gH$ and $hgah = ga$ for any $a \in H$. Consequently, $h \in H$, $hg = gh^{-1}$, $g^{-1}hga = ah^{-1}$ and $h^{-1}a = ah^{-1}$ for all $a \in H$. □

COROLLARY 5.7. *If f is a transposition on G, then $6n - 24 \leqslant m_f \leqslant 6n - 8$. Moreover, a transposition f with $m_f = 6n - 24$ exists iff there exist $g, h \in G$ with $gh = hg$, $h^2 = 1$ and $g \neq 1 \neq h$, $g \neq h$.*

PROOF. Let $f = (g\, b)$ be a transposition with $m_f = 6n - 24$. By 5.5(i) there exists $h \in G$ with $Lh = L$ for $L = \{g, b\}$. Therefore $H = \{1, h\}$ is a subgroup of G and 5.6 may be applied. □

PROPOSITION 5.8. *Let G be a finite group of order n and f a transposition on G. We can put $f = (a\, b)$ so that $a = 1$ or $b^2 = a$ or $b^2 \neq a \neq 1 \neq b \neq a^2$. Then $m_f = 6(n - 4) + \delta$, $0 \leqslant \delta \leqslant 16$, and exactly one of the following cases applies (we put $h = a^{-1}b$)*:
(i) *$a = 1$ and $b^2 = 1$. Then $\delta = 16$.*
(ii) *$a = 1$ and $b^2 \neq 1$. Then $\delta = 13$.*
(iii) *$b^2 = a \neq 1$ and $b^3 = 1$. Then $\delta = 6$.*
(iv) *$b^2 = a \neq 1$ and $b^3 \neq 1$. Then $\delta = 7$.*
(v) *$ab = ba$, $b^2 \neq a \neq 1 \neq b \neq a^2$ and $h^2 = 1$. Then $\delta = 0$.*
(vi) *$ab \neq ba$, $a \neq 1 \neq b$ and $h^2 = 1$. Then $\delta = 4$.*

(vii) $ab = ba$, $b^2 \neq a \neq 1 \neq b \neq a^2$ *and* $h^2 \neq 1$. *Then* $\delta = 6$.
(viii) $ab \neq ba$, $a \neq 1 \neq b$, $h^2 \neq 1$ *and* $a^2 = b^2$. *Then* $\delta = 6$.
(ix) $ab \neq ba$, $a \neq 1 \neq b$, $h^2 \neq 1$ *and* $a^2 \neq b^2$. *Then* $\delta = 8$.

PROOF. Using 5.1 and 5.3, m_f can be directly computed in each of the above cases. This is of an elementary nature, and hence it is omitted here. Note that (i) follows from 5.5(ii) and (v) from 5.7. Conversely, 5.8 provides another proof of 5.7.

REMARK 5.9. For n odd, only the cases (ii), (iii), (iv), (vii) and (ix) can occur.

6. MAIN RESULT

Let O be a finite non-trivial commutative group of an odd order. Denote by $D(O)$ the non-commutative group defined on $O \times \mathbf{Z}_2$ by $(a, 0) \cdot (b, h) = (ab, h)$, $(a, 1) \cdot (b, h) = (ab^{-1}, 1 + h)$. $D(O)$ is thus the semi-direct product of O and $\mathbf{Z}_2$ induced by the automorphism $a \to a^{-1}$ of O. If k is the order of O, then $D(O)$ contains k involutions and a normal group isomorphic to O. The dihedral group D_{2k} is isomorphic to $D(\mathbf{Z}_k)$.

We now define $\delta_0(G)$ for each finite group G of an order $n \geq 5$. We put $\delta_0(G) = 6n - 18$ if n is odd, $\delta_0(G) = 6n - 20$ if $G \simeq D(O)$ for a non-trivial commutative group O of an odd order, and $\delta_0(G) = 6n - 24$ in the remaining cases.

PROPOSITION 6.1. *Let G be a finite group of an order $n \geq 5$. Then there exists a transposition f of G with $m_f = \delta_0(G)$. Furthermore, $m_f \geq \delta_0(G)$ for any transposition f of G. Finally, if $n \geq 12$, and f is such a permutation of G that $n > \operatorname{card}\{a \in G; f(a) = a\} > 2n/3$, then $m_f \geq \delta_0(G)$ and f is a transposition whenever $m_f = \delta_0(G)$.*

PROOF. First, we shall make clear that there exist $a, b \in G$ satisfying the appropriate case (i)–(ix) of 5.8, and that no case exhibiting smaller distance applies to G. If $b \in G$ is an element of order 3, then b and $a = b^2$ satisfy (iii). If $c \in G$ is an element of an order greater than 3, then $a = c$, $b = c^3$, or $a = c^2$, $b = c^3$ satisfy (vii). Together with 5.9 this settles the case when n is odd. If $h^2 = 1$, $1 \neq h \in G$ and $n > 2$, choose any $a \in G$ with $1 \neq a \neq h$ and put $b = ha$. Then (v) applies if $ah = ha$, and (vi) applies in the opposite case. If G contains a subgroup H of order 4, then a and h can be chosen from H, and we have $ah = ha$. Now suppose that $n = 2r$, $r > 1$ is odd, and $hg \neq gh$ whenever $h^2 = 1$, $1 \neq g \neq h \neq 1$. Then G acts transitively and faithfully on the set of all its involutions I by the conjugation, and as $g^{-1}hg = h$ implies $g = 1$ or $g = h$ for any $h \in I$, $g \in G$, we see that G is in fact a Frobenius group of degree r. If O is its regular normal subgroup, then O is commutative and $G \simeq D(O)$ by [6, Proposition I.8.3].

Now assume that $n \geq 12$, f is a permutation of G and $n > k = \operatorname{card}\{a \in G; f(a) = a\} > 2n/3$. We have just proved that $m_f \geq \delta_0(G)$ if f is a transposition. Hence we can assume $n > l = n - k \geq 3$. By 5.4, $m_f > \delta_0(G)$ if $3ln - 6l^2 > \delta_0(G)$. This clearly holds for $l = 3$, $n \geq 12$, and for $n \geq 14$ we have $\delta_0(G) < n^2/3 = 3(n/3)n - 6(n/3)^2$. From this we conclude that $3ln - 6l^2 > \delta_0(G)$ for any $n/3 \geq l \geq 3$, if $n \geq 14$. As we have assumed $n > 3l$, only the case $n = 13$, $l = 4$ remains to be considered. In that case $\delta_0(G) = 3ln = 6l^2 = 60$. As 13 is a prime, no $L \subsetneq G$ with $2 \leq \operatorname{card}(L) = l < 13$ can satisfy $Lh = L$ for $h \neq 1$, and we obtain $m_f > 60 = \delta_0(G)$ from 5.5(i).

THEOREM 6.2. *Suppose that $G(\cdot)$ is a finite group of order $n \geq 5$, $G(*)$ another group on G and $m = \operatorname{dist}(G(\cdot), G(*)) > 0$. Then either $m > n^2/9$, or $m \geq \delta_0(G(\cdot))$. It holds that $\delta_0(G(\cdot)) < n^2/9$ whenever $n \geq 51$, and $\delta_0(G(\cdot)) > n^2/9$ for $n \leq 49$. The groups $G(\cdot)$*

and $G(*)$ are isomorphic if $m \leq n^2/9$, and for any $G(\cdot)$ there exists group $G(*)$ isomorphic to $G(\cdot)$ such that $m = \delta_0(G(\cdot))$.

PROOF. First, verify that $\delta_0(G(\cdot)) < n^2/9$ for $n \geq 51$ and $\delta_0(G(\cdot)) > n^2/9$ for $n \leq 49$. If $m \leq n^2/9$, then $m \geq \delta_0(G(\cdot))$ by 4.5 and 6.1. The rest follows from 4.5 and 6.1 as well.

COROLLARY 6.3. *$\delta(G(\cdot)) = \delta_0(G(\cdot))$ for $n \geq 51$.*

7. NON-ISOMORPHIC GROUPS

LEMMA 7.1. *Suppose that H and K are finite groups of the respective orders h and k, and that $\Psi: H \to \mathrm{Aut}(K)$, $\Psi(a) = \psi_a$ is a group homomorphism. Let t denote the number of orbits of the group $\Psi(H)$ acting on K and let $G(\cdot) = K \times H$. Furthermore, let $G(*)$ be the semi-direct product of K and H induced by Ψ, i.e. $(k_1, h_1) * (k_2, h_2) = (k_1 \psi_{h_1}(k_2), h_1 h_2)$ for any $(k_i, h_i) \in G$, $i = 1, 2$ and let $n = hk = \mathrm{card}(G)$. Then $m = \mathrm{dist}(G(\cdot), G(*)) = n^2 - nth$, and $m > 0$ iff $\Psi(H) \neq 1$. Suppose that $m > 0$ and denote by q the least prime dividing h, and by p the least prime dividing k. Then $m \geq n^2(p-1)(q-1)/pq \geq n^2/4$.*

PROOF. The number of points fixed by the permutations of a permutation group is equal to the product of the group order and the number of orbits (e.g., see [6, Proposition I.3.1.]). Therefore $th = \mathrm{card}\{(b, a) \in K \times H;\ \psi_a(b) = b\}$ and $m = n^2 - nth = n^2(1 - t/k)$. Elements of K fixed by all ψ_a, $a \in H$ form a subgroup of K of an order $r \neq k$. Denote its index by i; then $k = ri$ and $i \geq p$. Each orbit of $\Psi(H)$ with at least two points contains at least q points. Hence $t \leq r + (k - r)/q = k(q + i - 1)/qi \leq k(q + p - 1)/qp$ and $n^2(1 - t/k) \geq n^2(p-1)(q-1)/pq$.

EXAMPLE 7.2. For $n = 2p^2 r$, $p > 1$, put $H = \mathbf{Z}_2$, $K = \mathbf{Z}_p \times \mathbf{Z}_p \times \mathbf{Z}_r$ and $\psi_1((a, b, c)) = (b, a, c)$ for any $(a, b, c) \in K$. Then $t = r(p^2 + p)/2$ and $\mathrm{dist}(G(\cdot), G(*)) = n^2(p-1)/2p$.

EXAMPLE 7.3. Consider the Abelian group $G(+) = \mathbf{Z}_h \times \mathbf{Z}_k$, $h \geq 2$, $k \geq 2$ and define a cyclic group $G(\cdot)$ so that $(1, 0)^s = (i, j)$ whenever $s = i + jh$, $0 \leq i \leq h - 1$, $0 \leq j \leq k - 1$. Then $(h_1, k_1) \cdot (h_2, k_2) = (h_1 + h_2, k_1 + k_2)$ iff $h_1 + h_2 < h$, and hence $\mathrm{dist}(G(+), G(\cdot)) = n^2(h-1)/2h \geq n^2/4$.

EXAMPLE 7.4. Let $H(\cdot)$ and K be finite groups of the respective orders h and k, $hk = n$. Suppose that $H(*)$ is another group on H and let $\mathrm{dist}(H(\cdot), H(*)) = rh^2$, $0 \leq r \leq 1$. Put $G(\cdot) = H(\cdot) \times K$ and $G(*) = H(*) \times K$. Then $(h_1, k_1) * (h_2, k_2) \neq (h_1 h_2, k_1 k_2)$ iff $h_1 * h_2 \neq h_1 h_2$, and hence $\mathrm{dist}(G(\cdot), G(*)) = rn^2$.

CONJECTURE 7.5. Let G be a finite group of order n and p the least prime dividing n. Then $v(G) \geq n^2(p-1)/2p$.

8. THE INFINITE CASE

In this section let $G(\cdot)$ and $G(*)$, $G(\cdot) \neq G(*)$ be two infinite groups with the same underlying set G, $\mathrm{card}(G) = \kappa$.

LEMMA 8.1. *If $(a, b) \in M$, then $\max(p_1(a), p_1(b), p_1(ab)) = \max(p_2(a), p_2(b), p_2(ab)) = \max(p_3(a), p_2(b), p_3(ab)) = \max(p_1(a), p_3(b), p_3(ab)) = \kappa$.*

PROOF. Proceed similarly as in the proof of 2.4. □

COROLLARY 8.2. *If* $G(\cdot) \neq G(*)$, *then* $\operatorname{dist}(G(\cdot), G(*)) = \kappa$.

PROPOSITION 8.3. *Let* $G(\cdot)$ *and* $G(*)$ *be two infinite groups with* $\operatorname{card}(G) = \kappa$, *and let* $L = \{a \in G; p_1(a) = \kappa\}$. *If* $\operatorname{card}(L) < \kappa$, *then there exists a unique isomorphism* $f: G(\cdot) \to G(*)$ *with* $f(ab) = a * b$ *for any* $a, b \in K = G \setminus L$. *Moreover,* $f(a) = a$ *iff* $a \in K$.

PROOF. First, note that $\operatorname{card}(\bigcap K_i) = \kappa$, $1 \leqslant i \leqslant 4$ whenever $K_i \subseteq G$ and $\operatorname{card}(G \setminus K_i) \leqslant \operatorname{card}(L)$. Furthermore, it follows from 8.1 that $ab = a * b$, if $\{a, b, ab\} \subseteq K$. By induction $a_1 a_2 \cdot \cdot \cdot a_k = a_1 * a_2 * \cdot \cdot \cdot * a_k$ whenever $a_i \in K$, $1 \leqslant i \leqslant k$ are such that $a_1 a_2 \cdot \cdot \cdot a_i \in K$ for any $2 \leqslant i \leqslant k$. Each $g \in G$ can be expressed κ times as a product $g = ab$, $a, b \in K$. If $g = a_i b_i$, $1 \leqslant i \leqslant 2$, $a_i, b_i \in K$, then we can show that $a_1 * b_1 = a_2 * b_2 = f(g)$ in the same way as in step (iv) of proof 2.1. The steps (v)–(vii) can be repeated with little change. To see that f is surjective, note that any $g \in G$ can be expressed as $g = a * b$, $a, b \in K$. It remains to prove that $f(g) \neq g$ for $g \in L$. Assume the contrary. Then there exists $b \in K$, with $gb \in K$ and $g * b \neq gb$. Therefore $gb = f(gb) = f(g) * f(b) = f(g) * b \neq g * b$, and hence $f(g) \neq g$.

ACKNOWLEDGEMENT

The author wishes to thank the referees for valuable comments concerning the presentation of the first version of this paper. He also thanks to one of the referees for pointing out that $\mu(G(\cdot))$ was computed incorrectly for the special case of $n = 6$ in both [1] and [2].

REFERENCES

1. J. Dénes, On a problem of L. Fuchs, *Acta Sci. Math. (Szeged)*, **23** (1962), 237–241.
2. J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest, 1974.
3. J. Dénes, and A. D. Keedwell, *Latin Squares: New Developments in the theory and Applications*, North Holland, Amsterdam, 1991.
4. A. Drápal, On quasigroups rich in associative triples, *Discr. Math.*, **44** (1983), 251–265.
5. M. Hall and L. J. Paige, Complete mappings of finite groups, *Pac. J. Math.*, **5** (1955), 541–549.
6. D. S. Passman, *Permutation Groups*, W. A. Benjamin, New York, 1968.

Received 22 February 1991 and accepted in revised form 10 February 1992

ALEŠ DRÁPAL
Department of Mathematics,
Charles University,
Prague, Czechoslovakia